

FORM PTO-1300
(REV 12-29-99)

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER

TRANSMITTAL LETTER TO THE UNITED STATES
DESIGNATED/ELECTED OFFICE (DO/EO/US)
CONCERNING A FILING UNDER 35 U.S.C. 371

BO 41539

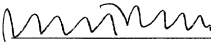
097509983
OFFICE OF THE INTERNATIONAL BUREAU (37 CFR 1.5)INTERNATIONAL APPLICATION NO.
PCT/NL98/00581INTERNATIONAL FILING DATE
09 OCTOBER 1998PRIORITY DATE CLAIMED
10 OCTOBER 1997TITLE OF INVENTION
METHOD AND DEVICE FOR PROTECTING DATA COMMUNICATIONAPPLICANT(S) FOR DO/EO/US
Ralph Rogier DE LA BRETONIERE

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
 - a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☐ has been transmitted by the International Bureau.
 - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
 - a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☐ have been transmitted by the International Bureau.
 - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
 - d. ☐ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.
☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information: International Preliminary Examination Report
International Search Report
Verified Statement Claiming Small Entity Status
Patent Data Entry Sheet

U.S. APPLICATION NO. 097509983 INTERNATIONAL APPLICATION NO. PCT/NL98/00581	ATTORNEY'S DOCKET NUMBER BO 41539																
17. <input checked="" type="checkbox"/> The following fees are submitted: BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) : Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO \$970.00 International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO \$840.00 International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO \$690.00 International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) \$670.00 International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) \$96.00 <div style="text-align: center;">ENTER APPROPRIATE BASIC FEE AMOUNT =</div>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="text-align: left;">CALCULATIONS</th> <th style="text-align: left;">PTO USE ONLY</th> </tr> <tr> <td style="height: 40px;"></td> <td></td> </tr> <tr> <td style="text-align: right;">\$ 840</td> <td></td> </tr> </table>	CALCULATIONS	PTO USE ONLY			\$ 840											
CALCULATIONS	PTO USE ONLY																
\$ 840																	
Surcharge of \$130.00 for furnishing the oath or declaration later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(e)).																	
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="text-align: left;">CLAIMS</th> <th style="text-align: left;">NUMBER FILED</th> <th style="text-align: left;">NUMBER EXTRA</th> <th style="text-align: left;">RATE</th> </tr> <tr> <td>Total claims</td> <td>9 - 20 =</td> <td>0</td> <td>X \$18.00</td> </tr> <tr> <td>Independent claims</td> <td>2 - 3 =</td> <td>0</td> <td>X \$78.00</td> </tr> <tr> <td colspan="3"></td> <td>+ \$260.00</td> </tr> </table>	CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	Total claims	9 - 20 =	0	X \$18.00	Independent claims	2 - 3 =	0	X \$78.00				+ \$260.00	
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE														
Total claims	9 - 20 =	0	X \$18.00														
Independent claims	2 - 3 =	0	X \$78.00														
			+ \$260.00														
MULTIPLE DEPENDENT CLAIM(S) (if applicable)																	
TOTAL OF ABOVE CALCULATIONS =																	
Reduction of 1/2 for filing by small entity, if applicable. A Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28).																	
SUBTOTAL =																	
Processing fee of \$130.00 for furnishing the English translation later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(f)).																	
TOTAL NATIONAL FEE =																	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). \$40.00 per property																	
TOTAL FEES ENCLOSED =																	
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 60%;">Amount to be refunded:</td> <td style="width: 40%;">\$</td> </tr> <tr> <td>charged:</td> <td>\$</td> </tr> </table>		Amount to be refunded:	\$	charged:	\$												
Amount to be refunded:	\$																
charged:	\$																
a. <input checked="" type="checkbox"/> A check in the amount of \$ <u>420.</u> to cover the above fees is enclosed.																	
b. <input type="checkbox"/> Please charge my Deposit Account No. _____ in the amount of \$ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.																	
c. <input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge any additional fees which may be required by 37 CFR §1.16 and 1.17, or credit any overpayment to Deposit Account No. 25-0120. A duplicate copy of this sheet is enclosed.																	
NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.																	
SEND ALL CORRESPONDENCE TO: YOUNG & THOMPSON 745 South 23rd Street Second Floor Arlington, VA 22202 CUSTOMER NO. 000466 Tel. (703)521-2297 Fax (703)685-0573	April 5, 2000 <div style="text-align: right;">  SIGNATURE: <u>Robert J. Patch</u> NAME <u>17,355</u> REGISTRATION NUMBER </div>																

Form A

**VERIFIED STATEMENT CLAIMING SMALL ENTITY STATUS
(37 CFR 1.9(f) & 1.27(b))--INDEPENDENT INVENTOR**

Docket Number (Optional)

BO 41539

Applicant or Patentee: DE LA BRETONIERE, Ralph Rogier

Serial or Patent No.: _____

Filed or Issued: _____

Title: Method and device for protecting data communication

As a below named inventor, I hereby declare that I qualify as an independent inventor as defined in 37 CFR 1.9(c) for purposes of paying reduced fees to the Patent and Trademark Office described in:

- ☒ the specification filed herewith with title as listed above.
☐ the application identified above.
☐ the patent identified above.

I have not assigned, granted, conveyed or licensed and am under no obligation under contract or law to assign, grant, convey or license, any rights in the invention to any person who would not qualify as an independent inventor under 37 CFR 1.9(c) if that person had made the invention, or to any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(e).

Each person, concern or organization to which I have assigned, granted, conveyed, or licensed or am under an obligation under contract or law to assign, grant, convey, or license any rights in the invention is listed below:

- ☒ No such person, concern, or organization exists.
☐ Each such person, concern or organization is listed below.

Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

DE LA BRETONIERE, Ralph Rogier

NAME OF INVENTOR

NAME OF INVENTOR

NAME OF INVENTOR

Signature of inventor

Signature of inventor

Signature of inventor

Date

3 April

Date

Date

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of
Ralph Rogier DE LA BRETONIÈRE
Serial No. (unknown)
Filed herewith
METHOD AND DEVICE
FOR PROTECTING
DATA COMMUNICATION

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Prior to the first Official Action and calculation of the filing fee, please replace specification pages 1-5, as originally filed, with pages 1-5a as filed in the Article 34 amendment of 17 January 2000.

Please also replace Claims 1-10 as originally filed, which appear on pages 10 and 11, with Claims 1-9, also filed in the Article 34 amendment of 17 January 2000. The replacement specification pages and the pages containing amended Claims 1-9 are marked "AMENDED SHEET" and are attached hereto. Following the insertion of Claims 1-9, please amend these claims as follows:

IN THE CLAIMS:

Claim 3, line 1, change "one of the preceding claims," to --claim 1,--.

Claim 6, line 1, cancel "or 5".

Ralph Rogier DE LA BRETONIÈRE

Claim 8, line 1, cancel "or 5".

Claim 9, line 1, change "one of Claims 4 to 8," to
--Claim 4,--.

R E M A R K S

The above changes in the specification and claims merely place this national phase application in the same condition as it was during Chapter II of the international phase, with the multiple dependencies being removed. Following entry of this amendment by substitution of the pages, only amended claims 1-9 remain pending in this application.

Respectfully submitted,

YOUNG & THOMPSON

By



Robert J. Patch
Attorney for Applicant
Registration No. 17,355
745 South 23rd Street
Arlington, VA 22202
Telephone: 703/521-2297

April 5, 2000

09/509983

Method and device for protecting data communication

020 000 00 APR 2000

The invention relates to a method and a device for protecting data communication traffic through a communication link between a first communication station and a second communication station, in which the data is dispatched according to a data protocol from the second communication station to the first communication station, comprising the steps of (i) receiving the data from the second communication station in a data communication protection device and (ii) comparing the data protocol of the data with at least one standardised protocol in the data communication protection device. In particular, data communication links are protected which can be seized by third parties by means of public and/or private data and telecommunication infrastructure.

Furthermore, the present invention relates to a data communication protection device arranged for protecting data communication traffic between a first communication station and a second communication station, data being dispatched according to a data protocol from the second communication station to the first communication station, the data communication protection device comprising memory means for storing data characteristics of at least one standardised protocol, the data communication protection device further being arranged for comparing the data protocol of the data with the at least one standardised protocol.

Such a method and device are known from US-A-5,124,984, which discloses a method for protecting data communication traffic between a first communication station and a second communication station, in which the data is dispatched according to a data protocol from the second to the first communication station, in which the data protocol is compared with at least one standardised protocol and data is forwarded to the first communication station only when the data protocol complies with the at least one standardised protocol. The disclosed method and system are directed to data networks, the network interconnecting a number of stations and a network access controller. The network access controller is connected to the network and listens in on the data traffic on the network. The network access controller checks the content of each data package sent on the network and determines whether the packet is of an authorised type. It relies on control mechanisms present in the protocol that is being used in order to terminate communications between specific stations. It is disclosed that the network access controller is not part of the physical path between communication stations.

Appliances are found to an increasing extent on the market which are provided with an option which makes it possible to provide so-called remote service. This involves, in particular, installed fax equipment, network fax equipment, telephone modems, cable modems, combined fax/modem configurations, telephone sets, answering machines,

AMENDED SHEET

telephone exchanges, copying machines, washing machines and other domestic, industrial appliances and operating appliances which can communicate with one another via the said infrastructures. This relates to appliances which are installed separately and also in combination with other equipment. This remote service, also known as "remote diagnostics" or "remote maintenance" has been developed in order to be able to deliver a flexible and cheap method of support to the (end) users of the equipment.

Remote service, furthermore referred to as RDS ("Remote DiagnosticS") makes it possible to subject the respective appliance to an analysis via the said infrastructure from the location of the supplier or another service point. In a number of cases, it is even possible for the service engineer to be able to carry out small repairs remotely. If it emerges that repair has nevertheless to be carried out at the location of the appliance, the respective maintenance engineer or technician can be sent out with the correct components. Specifically, it is already known via RDS what is wrong with the appliance and what measures have to be taken to remedy the fault.

The functionality of RDS may comprise many advanced options:

- The reading-out of the various counter positions; when a service is necessary can be determined by interpreting the counter positions.
- The switching-on and switching-off of the visual and audible signals, for example, in the case of a fax machine; as a result it is possible to analyse the appliance remotely without disturbing the immediate environment.
- The reading-out of a fax/telephone number list; in the event of an alteration of (service) telephone numbers, these can be altered remotely.
- The reading-out of a fax log; the log usually contains the error codes of the last fax messages sent and these can be used by the technical support for the purpose of analysing the appliance.
- The manipulation of the fax memory; this is intended to offer a final possibility for erasing the memory if this is not possible by means of the prescribed manner.
- The alteration of the configuration settings; as a service, the appliance can be configured remotely in accordance with the wishes of the client.
- The adding of connecting-through numbers; the service centre can then examine any damaged faxes itself and infer therefrom what the possible cause of the fault is.

Although the functionality mentioned is concentrated on fax machines, a comparable functionality may be present in the other equipment mentioned above. The RDS functionality can, in principle, comprise all the functionality which relates to operations concerning the memories (RAM, ROM, EEPROM) present in the appliance.

5 Many manufacturers of data communication devices make use of so-called custom chip sets (standard integrated circuits produced in large numbers) or accommodate hardware produced in large numbers and delivered to many manufacturers in a separate housing. The specifications of the manufacturer will, in many cases, describe only the functions desired by the manufacturer. It is therefore possible that (RDS) functionality is
10 present in custom chip sets or hardware which is not made known to the end user.

In the modern information society, knowledge is power. Information is, of course, well protected by means of physical and organizational protection measures of all kinds. Documents may, for example, be seen only by a select group of individuals, after
15 which they are securely stored in the safe. For the purpose of rapid decision-making and refreshing the information situation, consultation will often be made by telephone, in which case use is frequently made of the fax machine to transmit the documents to be discussed to one another. It is here that there is a weak point in the entire security chain. Essentially, the respective documents are made available to third parties, the intention
20 being precisely to avoid that. Said third parties, who possibly have direct business interests or operate in the world of information brokerage, may acquire possession of valuable information. This may take place even without the owner of the sensitive information even having any indication until it is too late. The industrial spy therefore appears to be very near at hand and works, it is to be noted, together with the individual who has protected his own information with every means.

25 A fax machine has, for example, RDS functionality, whether this is known to the end user or not, and can thereby be manipulated by a third party. Said third party can ensure, for example, that the respective fax machine responds to certain fax numbers and/or fax identification numbers. During the transmission and/or reception of faxes from/to these fax numbers, the fax machine will transmit, for example, an additional copy
30 to the fax number specified by said third party. The user of the fax machine does not, however, notice anything in this case because the visual and audible signals can be switched off, the so-called fax through-connection number does not have to figure in the list of fax through-connection numbers and even the fax log does not have to report this

AMENDED SHEET

operation. If necessary, a copy of the fax involved is transmitted only during the night hours when no-one is present in the company.

In the case of a network fax or a modem fax incorporated in a network system within a company, it is conceivable that a third party obtains access via said fax or said modem to the network system. As a result, it might be possible also to extract information in the manner mentioned above from the network system, which is believed to be safe.

The object of the present invention is to provide a method and a device for protecting data communication traffic in order to prevent third parties being able to make unnoticed use of functionality present in a communication station.

According to the invention, the object is achieved by means of a method of the type defined in the introduction, characterized by the steps of (iii) providing the data communication protection device in the communication link, the data from the second communication station to the first communication station passing through the data communication protection device and (iv) forwarding data of which the data protocol complies with the at least one standardised protocol from the data communication protection device to the first communication station, and not forwarding data of which the data protocol does not comply with the at least one standardised protocol from the data communication protection device to the first communication station.

Repetitions of commands, or certain combinations of commands, which each belong per se to the standardized protocol but do not lead to normal, effective data communication traffic, are deemed not to belong to the standardized protocol. Specifically, it is possible that such repetitions or combinations of commands are used to switch on certain RDS functionality.

Before a fax machine, for example, can proceed to the reception and/or transmission of documents, the appliances at both ends of the communication link have to inform one another about the status they are in. After this so-called "handshake" procedure, the information exchange is mutually adapted. Both appliances are now ready and will carry out the desired task. This procedure and the information exchange proceeds according to internationally specified standards, also referred to as protocols, which are specified in part in the so-called ISO, ETSI and ANSI standards or in the ITU regulations. Before, during or after the "handshake" procedure, a check can take place on the presence of certain RDS functionality. To use RDS functionality, a manufacturer will use protocols which are not (entirely) incorporated in the standards. This means that the use of a so-called exotic protocol can indicate the use of RDS functionality. It indicates in any case

AMENDED SHEET

that the other party is not adhering to the standard protocols. The negation of the standard indicates that the link made is being used in a manner other than that which the user intended.

As a result of using the method according to the invention, an attempt of a
5 third party to switch on (concealed) RDS functionality from the outside will be unsuccessful, as a result of which the probability that information can leak out via the communication equipment used becomes substantially smaller.

Because, according to the invention, the data protocol is compared with standardized protocols, the method according to the invention can be used worldwide.

10 In an embodiment of the method according to the invention, the user of a communication station is warned if it emerges during the comparison of the data protocol that the latter does not belong to a known standardized protocol. As a result, the user is warned of an attempt of a third party to manipulate his communication station, whereupon the user can take direct action.

15 In a further embodiment of the method according to the invention, the link is interrupted if it emerges during the comparison of the data protocol that the latter does not belong to a standardized protocol. This has the result that any attempt to manipulate the communication station by a third party will be unsuccessful.

20 In a preferred embodiment of the method according to the invention, after ascertaining that the data protocol does not belong to a certain standardized protocol, a data file containing data of the data communication traffic and the second communication station is prepared. As a result of recording said data, the user is enabled to obtain as complete a picture as possible of the user of the second communication station, after which appropriate measures can be taken.

25 Another aspect of the invention provides a device suitable for carrying out the method according to the invention as defined in the preamble of claim 4. For this purpose, the device is further provided with a first link for linking the data communication protection device to the first communication station, and a second link for linking the data communication protection device to the second communication station, the data passing from
30 the second communication station to the first communication station through the data communication protection device and comparison/forwarding means for forwarding data received through the second link of which the data protocol complies with the at least one standardised protocol from the data communication protection device through the first link, and not forwarding data of which the

AMENDED SHEET

data protocol does not comply with the at least one standardised protocol from the data communication protection device through the first link.

With the device according to the invention, it is possible to use the abovementioned method in a data communication environment. An advantage of the device according to the invention is that the user can determine himself, regardless of the brand and type of appliance, whether RDS functionality is permitted. Because the device can be used separately from the local communication station, there is no need to pay attention to any RDS functionality present when purchasing the local communication station.

As a result of the small number of components required, it is possible to manufacture the device in a compact, lightweight and robust form and to adapt it to the situation in which it is used. Furthermore, the operation and the connection of the device are simple.

Preferably, the memory means are designed as a ROM memory. As a result, it is impossible for the contents of the memory means to be manipulated during use, but it is still simple to adapt the device to the latest standardized protocols by replacing the ROM memory.

In an embodiment of the device, the device furthermore comprises warning means. If data is detected of which the data protocol does not comply with the at least one standardized protocol, the user is warned, for example by visual and/or audible warning means. As a result, the user will always be warned if an attempt is made to manipulate the first communication station, even if an attempt is made in these circumstances to switch off indications of the first communication station.

A further embodiment of the device according to the invention comprises display means linked to the comparison/forwarding means, the

WO 99/20024

PCT/NL98/00581

6

display means displaying data relating to the data communication traffic and the second communication station which are stored after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol. This can be implemented, for example, as a display screen on the device itself.

As an addition, the device can be provided, in a further embodiment, with input means linked to the comparison/forwarding means for inputting commands relating to the display of the data.

An alternative embodiment of the invention is to provide it with interface means instead of the display means and/or the input means. Said interface means ensure the exchange of data relating to the data communication traffic and the second communication station with an external processing device, which data are stored after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol. Said processing device may be, for example, a computer with which the data are processed further and can be displayed.

By means of the display of said data, the user is enabled to obtain as complete a picture as possible of the attempt to manipulate the local communication station, after which appropriate measures can be taken.

According to an embodiment of the invention, the device can be integrated with the local communication station.

The method and the device according to the invention will now be explained further by reference to the drawings.

Figure 1 shows a diagram of an embodiment according to the invention;

Figure 2 shows a flow chart of the method according to the invention.

Figure 1 shows a diagram of a preferred embodiment according to the invention in which the device 10 for protecting data communication traffic is linked to a first communication station 11 and a second communication station 12. The device 10 comprises comparison/forwarding means 15 which can communicate during operation both with the first communication station 11 and the second communication station 12. The device 10 furthermore comprises memory means 14 linked to the comparison/forwarding means 15. In the preferred embodiment of the invention shown, the device 10 furthermore comprises warning means 16, display means 17 and input means 18, all linked to the

WO 99/20024

7

PCT/NL98/00581

comparison/forwarding means 15. The communication stations 11 and 12 may be, for example, fax or copying machines provided with an RDS functionality.

- In the memory means 14, the characteristics of the data communication are stored according to at least one standardized protocol. The comparison/forwarding means 15 serve to compare the data protocol of data which the second communication station wishes to dispatch to the first communication station 11 and to forward only data of which the data protocol complies with the at least one standardized protocol to the local communication station 11.

- In the preferred embodiment shown, the device 10 also comprises warning means 16, which give a warning after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol. The figure indicates that the warning means 16 are implemented as a warning lamp. However, it is possible to use other visual or audible warning means for this purpose.

- In the preferred embodiment of the invention shown, the device 10 also comprises display means 17 for displaying data relating to the data communication traffic and the second communication station 12 which have been stored after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol. Furthermore, the device comprises input means 18 for inputting commands relating to the display of the data. It is possible, for example, to input commands to display only a certain portion of the data on the display means.

- In an embodiment of the invention not shown, the device 10 comprises, instead of the display means 17 and input means 18, interface means which can be linked to an external processing device. This processing device may be, for example, a computer with which the data can be processed further, stored and displayed.

- Figure 2 shows the flow chart of the method according to the invention. The method begins with the reception of data from the second communication station 12 in block 1. In decision block 2, the data protocol of the data received in block 1 is compared with the standardized protocol. If the data protocol complies with the at least one standardized protocol, the data is forwarded to the first communication station 11 in forwarding block 3. The method then returns to block 1 to check the further data received.

If the data protocol does not comply with the at least one

WO 99/20024

8

PCT/NL98/00581

standardized protocol, the method continues the procedure in warning block 4, in which the user is warned. The following step in the procedure comprises the interrupt block 6, in which the link to the second communication station is interrupted. In a preferred embodiment of the method according to the invention, in block 5, a data file is stored in which data of the data communication traffic and the second communication station are stored in parallel with warning block 4 and interrupt block 6.

Using the method and device shown in the figures for protecting data communication traffic, an attempt of a third party to switch on (concealed) functionality from the outside will be unsuccessful, as a result of which the probability that information can leak out via the communication equipment used becomes appreciably smaller.

As a result of warning the user and recording data relating to the data communication traffic and the second communication station 12, the user is enabled to obtain as complete a picture as possible of the user of the second communication station, after which appropriate measures can be taken.

An advantage of the device described is that the user can determine himself, regardless of the brand and type of appliance whether RDS functionality is permitted. Because the device can be used separately from the first communication station, there is no need to pay attention to any RDS functionality present when purchasing the first communication station. Of course, the device 10 can also be physically incorporated in the first communication station 11. In that case, the comparison/forwarding means 15 can form an integral component of a processor present in the first communication station 11.

As a result of the comparison of the data protocol of the received data with standardized protocols, the method according to the invention can be used worldwide.

As a result of the small number of components required, it is possible to manufacture the device in a compact, lightweight and robust form and to adapt it to the situation in which it is used. Furthermore, the operation and the connection of the device are simple.

If the memory means are designed as a ROM memory, it is impossible for the contents of the memory means 14 to be manipulated during use, but it is still simple to adapt the device to the latest standardized protocols by means of replacing the ROM memory.

Although the device has been described for the protection of

WO 99/20024

9

PCT/NL98/00581

data communication traffic between two communication stations, it is, of course, also possible to protect the data communication traffic between a plurality of communication stations, such as, for example, in a network environment.

CLAIMS

1. Method for protecting data communication traffic through a communication link between a first communication station (11) and a second communication station (12), in
5 which the data is dispatched according to a data protocol from the second communication station to the first communication station, comprising the steps of:
- (i) receiving the data from the second communication station (12) in a data communication protection device (10);
 - (ii) comparing the data protocol of the data with at least one standardised protocol in
10 the data communication protection device (10), characterised by
 - (iii) providing the data communication protection device (10) in the communication link, the data from the second communication station (12) to the first communication station (11) passing through the data communication protection device (10); and
 - (iv) forwarding data of which the data protocol complies with the at least one
15 standardised protocol from the data communication protection device (10) to the first communication station (11), and not forwarding data of which the data protocol does not comply with the at least one standardised protocol from the data communication protection device to the first communication station.
- 20 2. Method according to Claim 1, characterized in that, after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol, a warning is generated.
- 25 3. Method according to one of the preceding claims, characterized in that, after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol, a data file containing data of the data communication traffic and the second communication station (12) is stored.
- 30 4. Data communication protection device (10) arranged for protecting data communication traffic between a first communication station (11) and a second communication station (12), data being dispatched according to a data protocol from the second communication station to the first communication station, the data communication protection device comprising memory means (14) for storing data characteristics of at least one standardised protocol, the data communication protection device (10) further being

AMENDED SHEET

arranged for comparing the data protocol of the data with the at least one standardised protocol, characterised in that the data communication protection device (10) further comprises

- a first link for linking the data communication protection device (10) to the first communication station (11), and a second link for linking the data communication protection device (10) to the second communication station (12), the data passing from the second communication station to the first communication station through the data communication protection device;

- comparison/forwarding means (15) for forwarding data received through the second link of which the data protocol complies with the at least one standardised protocol from the data communication protection device (10) through the first link, and not forwarding data of which the data protocol does not comply with the at least one standardised protocol from the data communication protection device (10) through the first link.

15

5. Data communication device according to Claim 4, characterized in that the device furthermore comprises warning means (16) linked to the comparison/forwarding means (15) which give a warning after it has emerged during the comparison of the data protocol that it does not belong to the at least one standardized protocol.

20

6. Device according to Claim 4 or 5, characterized in that the device furthermore comprises display means (17) linked to the comparison/forwarding means (15), the display means (17) displaying data relating to the data communication traffic and the second communication station (12), which data are stored after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol.

25

7. Device according to Claim 6, characterized in that the device furthermore comprises input means (18) linked to the comparison/forwarding means (15) for inputting commands relating to the display of the data.

30

8. Device according to Claim 4 or 5, characterized in that the device comprises interface means for exchanging data relating to the data communication traffic and the

AMENDED SHEET

second communication station (12) with an external processing device, which data are stored after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol.

- 5 9. Device according to one of Claims 4 to 8, characterized in that the device (10) is integrated in the first communication station (11).

AMENDED SHEET

09/509983

WO 99/20024

PCT/NL98/00581

1/1

Fig 1

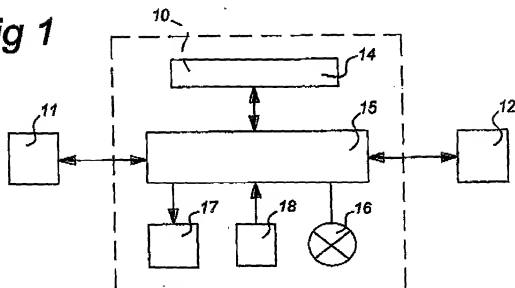
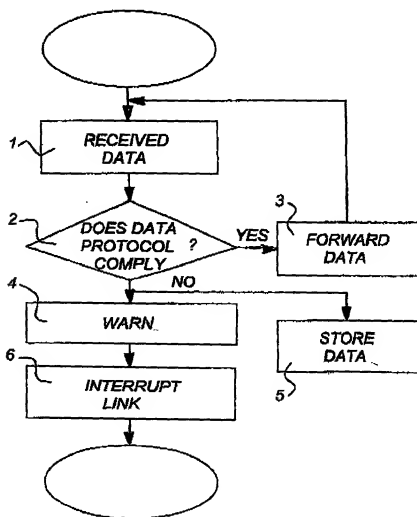


Fig 2



(complete (d) or (e))

- d. ☐ no such applications have been filed
 e. ☒ such applications have been filed as follows

**EARLIEST FOREIGN APPLICATION(S), IF ANY FILED WITHIN 12 MONTHS
 (6 MONTHS FOR DESIGN) PRIOR TO SAID APPLICATION**

Country	Application Number	Date of filing (day, month, year)	Date of Issue (day, month, year)	Priority claimed
Netherlands	1007252	October 10, 1997		Yes

**ALL FOREIGN APPLICATION(S), IF ANY FILED MORE THAN 12 MONTHS
 (6 MONTHS FOR DESIGN) PRIOR TO SAID APPLICATION**

CONTINUATION-IN-PART

(Complete this part only if this is a continuation-in-part application)

I hereby declare claim the benefit under Title 35, United States code, paragraph 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claim of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, paragraph 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, paragraph 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.) (Filing date) (Status) (patented, pending, abandoned)

(Application Serial No.) (Filing date) (Status) (patented, pending, abandoned)

POWER OF ATTORNEY

As a named inventor, I hereby appoint the following attorney(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: Robert J. PATCH, Reg. No. 17,355, Andrew J. PATCH, Reg. No. 32,925, Robert F. HARGEST, Reg. No. 25,590, Benoit CASTEL, Reg. No. 35,041, Eric Jensen, Reg. No. 37,855, and Thomas W. PERKINS, Reg. No. 33,027 c/o YOUNG & THOMPSON, Second Floor, 745 South 23rd Street, Arlington, Virginia 22202.

Address all telephone calls to Young & Thompson at 703/521-2297.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that wilful false statements and the like so made are punishable by fine or imprisonment, or both under Section 1001 of Title 18 of the United States Code and that such wilful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or first inventor: DE LA BRETONIERE, Ralph Rogier

Inventor's signature

Date: 2 April 2000

Country of Citizenship: the Netherlands

Residence: ZOETERMEER, The Netherlands

Post Office Address: Bijhouwerlommer 43, NL-2728 JK ZOETERMEER, The Netherlands

NLX

CHECK PROPER BOX(ES) FOR ANY ADDED PAGE(S) FORMING A PART OF THIS DECLARATION

COMBINED DECLARATION AND POWER OF ATTORNEY

(ORIGINAL DESIGN, NATIONAL STAGE OF PCT OR CIP APPLICATION)

As a below named inventor, I hereby declare that

My residence, post office address and citizenship are as stated below next to my name, I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

"Method and device for protecting data communication"

the specification of which: (complete (a), (b) or (c) for type of application)

REGULAR OR DESIGN APPLICATION

- a. ☐ is attached hereto.
b. ☐ was filed on _____ as Application
Serial No. _____ and was amended on _____
(if applicable)

PCT FILED APPLICATION ENTERING NATIONAL STAGE

- c. ☒ was described and claimed in international application No. Pct/NL98/00581
filed on October 9, 1998
and as amended on _____ (if any)

ACKNOWLEDGEMENT OF REVIEW OF PAPERS AND DUTY OF CANDOR

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, paragraph 1.56(a).

In compliance with this duty there is attached an information disclosure statement 37 CFR 1.97

PRIORITY CLAIM

I hereby claim foreign priority benefits under Title 35, United States Code paragraph 119 of any foreign application (s) for patent of inventor's certificate listed below and have also identified below any foreign application for patent of inventor's certificate having a filing date before that of the application on which priority is claimed.